June 13, 2022
RE: HJ 48 Draft Legislation

Chairman Bogner and Committee Members,

Thank you for your hard work over the last few months listening to stakeholders and considering policy changes regarding government's use of facial recognition technology. We appreciate your commitment to protecting Montanans' privacy.

In November, Frontier Institute had outlined two main privacy concerns with facial recognition technology (FRT) use by state and local governments:

1. **No uniform standard for the use of FRT by law enforcement**
2. **No uniform standard for accessing civilian FRT databases**

We recommended that the legislature consider adopting a transparent, uniform standard for FRT use by law enforcement in Montana. The uniform standard should establish the necessary legal conditions for investigations or searches which utilize FRT (reasonable suspicion, probable cause etc.). Standards should also protect the biometric data of law abiding Montanans by restricting law enforcement access to non-criminal FRT databases.

Based on these policy recommendations, Frontier Institute offers the following comments on key sections of the draft legislation that has been developed by the committee:

**Comment #1:** Section 7 restricts the use of FRT by state and local governments. Subsection 1 appears to prohibit the use of FRT for anything other than serious criminal searches or IDing a missing, endangered, or deceased person. This strict prohibition is not consistent with the intent of the legislature stated in Section 2 to "provide state and local government agencies the ability to use facial recognition services for limited uses including fraud prevention, probation services, and for certain criminal investigations."

Instead of prohibiting all government uses of FRT unless specifically allowed, consider reversing this provision: allow government agencies to use FRT unless the use is specifically prohibited or restricted. This would continue to allow Montana's governments to utilize FRT to assist in fraud prevention, identity verification and other beneficial uses while protecting the privacy rights of Montanans.

**Comment #2:** Section 7 raises the legal standard for state criminal investigations utilizing FRT. Currently, MATIC requires reasonable suspicion to authorize FRT per internal policy[1]. Under Section 7, law

---

[1] https://leg.mt.gov/content/Committees/Interim/2021-2022/Economic%20Affairs/Studies/HJR-48/February%20Meeting/MATIC-K-3-Facial-Recognition-Policy-2020.pdf

enforcement FRT searches would require probable cause. The legislature should consider carefully how this heightened standard would impact law enforcement operations.

**Comment #3**: Section 7 Subsection 3(a) requires law enforcement to submit a request to the criminal intelligence advisory council for authorization of a facial recognition search. This appears to be an unnecessary bureaucratic hurdle. The process to request a warrant should be sufficient to authorize law enforcement use of facial recognition for a criminal search.

**Comment #4**: Section 4 importantly sets standards for FRT systems used by state and local governments. However, this section could be improved by requiring all FRT systems used or third party vendors to verify proof of a warrant before biometric data stored in a FRT system is released to law enforcement as part of a criminal search. It also should prohibit government FRT systems from automatically sharing biometric data with external law enforcement databases (such as the DMV database's automatic uplink[2] to NLETS). This would bring Section 4 into alignment with Section 7, which requires a warrant for all criminal searches by law enforcement.

**Comment #5:** Drafters should consider giving special attention to continuous facial recognition surveillance in Section 7. Continuous facial recognition using footage captured or recorded by surveillance cameras to identify anyone who walks by, like that used by China to enforce dystopian social credit scores, is likely the most concerning use of government facial recognition technology from a privacy standpoint and should face the highest legal standards prior to deployment. This type of general surveillance should only be used in a discreet, targeted basis to identify specific individuals who are suspected of a crime, and only in the most urgent scenarios. Drafters should consider whether to restrict the amount of time and types of scenarios that continuous facial recognition surveillance can be authorized for.

Thank you for considering my comments and please reach out if I can be helpful during this process.

In Liberty,

Kendall Cotton
President and CEO

---

[2] https://leg.mt.gov/content/Committees/Interim/2021-2022/Economic%20Affairs/Studies/HJR-48/February%20Meeting/HJ48-Nlets-Followup-Questions.pdf